一份不负责任的登机指南

不见啦

2019 年 9 月 28 日

摘要

建议注册一个 GitHub 账号，建议注册一个 GitHub 账号。

这份文件是给部分觉得需要了解机场相关知识的人提供的，一份简单的，业余的说明文档。作者是一个普通的用户，因此不能保证文档的专业性，仅供参考。需要说明的是，本文档虽然列了很多软件，但严重缺失部分软件使用教程。

我并没有把自己定位到需要达到开发者理解的程度，只是从一个用户的身份出发，对一些可能接触到的概念做一些解释和说明。真要搞开发的话，你们可能就见不到我了。。。

因为手里只有 Android 和 Windows 设备，因此这两部分细节多些，iOS 的资料其实很多，很容易搜到。其他真的了解不足。

本人不对正确性做出保证，也不对由此引发的一切纠纷或其他负责，也不会再更新文档。

目录

1 机场的选择和使用

1.1 什么是机场

其实这个很好解释，我们常用的 SS/SSR 都是纸飞机的图标。所以我们有时也把这类软件和他们的衍生版叫做小飞机。而机场则可以认为是提供供这类软件服务的场所。大致是如此。

1.2 机场与自建

我看别人自建或是合租一个 VPS 也用的好好的，机场的优势在哪里呢？

有图

1.3 公益机场

有部分热心人士，会分享属于自己的节点信息，以自建居多。这些信息主要集中在 GitHub 和 TG 群组，使用体验有好有差，部分情况下会需要不断改变订阅链接，需要你仔细衡量你的需求/体验/成本。

1.4 白嫖机场

不做评价。

1.5 大致确定需求

详细概念请阅读第五部分：扩展模块。

简单来说，直连就看你脸，你的流量直接出国，过墙。中转使得出国相对更稳定一点，BGP 是中转的一种方式，有的过墙有的不过。IPLC（也称专线）不过墙，目前机场语境下的 IPLC 主要的是指阿里云内网。如深港即深圳阿里云–香港阿里云，点对点连接。线路需要落地，不同的落地决定了你可使用的互联网服务的不同。具体参考第五部分，落地。

通用语境下专线应该是物理专线。海缆走的流量的绝大部份是公网流量，极少部分是专线流量。

不同的线路决定了流量价格的不同，我还没好是否介绍线路特点。这部分可参考第五部分的倍率一节，有较为详细的解释。而他们的稳定性不同

（稳定性指服务的可用性/你国庆/六一想不想用），也因此最简单来说价格也就不一样了。

因此，你需要对你的使用场景和需求做一个评估，然后你才能去找寻相关人员进行套餐分析。但我也知道，你其实不知道你有什么需求。。。我会列一些常见的流量需求和机场常见的流量等级，请对自己的需求做一个评估。

已经作图了！这里就不写了。等我啥时候学会插入图片再修改。

1.6 获取机场链接

我大概明白自己的需求了，我要到哪里选择合适我的机场呢？

此处有毒药的机场介绍和毒药的 TG 群组 请带着你对上述问题的回答到上述链接的网站自行翻阅或加入群组进行讨论，得到相应的回复即可。

1.7 担心其一

我还是有点问题，我是个小白，我在这里该如何提问呢？我怕被人骂菜鸡。。。

如果你仔细看完了上边的问答，而且礼貌的话就没事。正常提出需求就行。那些群里的人也就是先来的用户而已，他们基本是使用者。你要是看完了第五部分倒是了解的比他们多了。只看 1.5 的简略版也够基本聊天了。//公共群一般都是吹水群，别太担心。

1.8 担心其二

我得到了推荐，我要如何判断他们的具体水准和合适我的程度呢？那些发链接和别人说的 aff 是什么意思？

这个只能看你对这些事务的接受程度，你选择采信毒药博客和群友在整体上处于独立状态下意见可靠性，就可以选择你相中的，进行购买尝试。初次购买，建议短期，但不一定要选最便宜的套餐，那你就没办法去评判机场的整体体验了。新机场部分在 1.9 有补充。

aff 是推广链接的缩写，机场希望发动自来水，促进人员增长。你这么聪明，一定明白了吧。这些 aff 可信吗？请参考上一问的关于可信度的回复。

1.9 担心其三

我还是有点担心，这些新机场值得信赖吗？他们会盗取贩卖我的个人隐私吗？

他人做事，除了极少数脑子抽的，都会考虑成本和收益。你觉得他们对你的这些信息的投入和所得会对等吗？同理也可以解释，为什么国家不抓个人翻墙，要抓也是抓机场主（笑

新机场处于扩张阶段，一般来说对新用户优惠多，节点会处在增加阶段，部分可能手忙脚乱的。//主要针对有毒药有提及和群友多人推荐的。//相对采信。

但在此处要注意，部分新站是有捞一笔就跑的打算的。一般来说，一切服务都跟成本挂钩，线路质量好，就不太容易跑路，全是直连的还可以随时结束服务的如 AWS，Azure，GCP 等，这些在非特殊时期或出于宣传，测速都会很好看，遇到类似这种情况的就需要你提高警惕了。有家宽，商宽或其他长期合同约束的落地，相对可靠性高于刚才提到的。

1.10 担心其四

我可以退款吗？有免费体验吗？机场跑路了怎么办？

能否退款以各机场自己的条款为准，一般注册/支付的时候都可以看见：不允许退款（笑

免费服务请注册后登录查看。

跑路啊，跑路那就。。。

跑路呗。。。

1.11 担心其五

为什么很多网站的界面那么相象呢？他们是同一家吗？

现在翻墙服务提供商遍地开花，你要是花钱，自己也能开一家。。。

好了，以上都是玩笑话。机场行业如今已经很成熟了。各级人群构成了一个体系完整，分工合作？的行业。有线路销售，有网站面板解决方案，有技术支持，有人负责黑别人，有代理。在 tg 群组里，你能看到形形色色的人，尤其是各种账号的贩卖和合租群。

机场的界面相似只是因为他们采用了相同的网站搭建方案。大部份网站使用了 sspanel，你可于页面底部可看到 staff 标识，点击即可查看有关信

息。如果要询问他人，注意礼貌。

1.12 担心其六

我登录了页面，发现没购买无法查看套餐，我要如何办呢？

一般来说，常见的你在这个指南里最常看到的是与毒药博客有关的信息。所以，基本你都可以在他的博客看到具体的价格和线路信息。缺少的部分细节，可于注册后查看，或加入对应的群组/公共群进行询问，一般很容易就会得到解答。

1.13 获取链接和注册购买

我下定了决心，选择了一家机场。请问，我如何进行购买和使用呢？

通常来说，在他人给你推荐的时候一般会给你相应的群组链接，群组地址或者你可以自行在毒药博客搜寻并打开。通常情况下建议你先关注毒药测速频道（网站有提供）浏览近期的消息，看是否有机场开放或关闭了注册。通常情况下建议你先通过上述的链接进入相应机场的群组，这样有问题可以及时得到反馈。

当你进入群组后，请点击置顶或群头像查看网站信息。点击进入并登录查看。注册账号并选购套餐或选购套餐然后注册，具体以网站为准。注意：通常情况下，注册而不购买套餐的账号都会在不久后被删除，部分网站即使充值而不购买套餐也会被删号，请仔细考虑。如你是通过邀请码 * 注册，请尽量不要浪费别人邀请名额。

我建议机场网址尽量在电脑打开，方便扫码支付。手机支付有时候需要截图，而微信还是支付宝会不支持扫码我也忘了。。。部分机场网站需要代理打开，但你已经登陆了 TG，这应该难不倒你。建议开启全局进行注册。支付的时候如果全局无法支付，请关闭代理。提示 *。// rix 支付网关有问题，出现 404。请尽情报错。。。

1.14 使用条款 1

好的，我支付完成了，我要如何进行使用呢？

请于注册后/前关注相应的机场频道或其他线路通知渠道，以便你及时获取节点变动，网站变动，订阅更新，优惠活动等信息。

其次，请仔细阅读机场的服务条款/TOS，请注意以下几项：对 BT/PT 的限制，对在线 IP 的限制，严禁合租/转卖/泄露账号、配置信息、IP/域名等，其他自行参考。如有泄露，请立即删除并重置订阅链接。一般情况下，订阅仅限个人使用，团体使用请购买团体套餐/单独注册。

出现问题，请参考机场的要求，是工单，群里提问还是其他。请注意：机场一般仅提供有限的技术支持，但一般都当了保姆。。。

因违反条款而导致账号被封禁，由你本人承担一切责任。

1.15 使用条款 2

我可以分享给我的朋友使用吗？他只偶尔用用/你们允许合租吗？

具体请以你的套餐为准，如你购买的为单人套餐，请仔细重新阅读 TOS，是不允许进行分享的。如果你进行分享了，则可能被系统检测到进而导致账户被封禁。到时候也许你和管理求情可以获得解封，可这毕竟是额外的操作，再说如果人家不给你解封也是没问题的。还是尽可能减轻自己使用的麻烦算了。如果你的朋友想要使用，你可以进行邀请购买，这样你也可以获得返利，可用在下一次的续费。

至于合租则是严厉禁止，这个比刚才提到的情况抓的还严，封禁了你基本不太有机会解封。不要为了他人使自己惹到了麻烦。

1.16 其他 1

节点信息的获取

一般来说，都在你的个人中心–产品服务–激活的服务，点击查看。查看订阅方式，软件支持等。

并首先参考机场本身的文档和订阅链接进行操作。其他可部分参考我的第三部分或自行研究。

1.17 其他 2

部分代理软件需要付费下载，部分机场提供了下载方式后下载说明。请遵照指示进行操作。

如不提供，请自行购买，如淘宝/官网/自注册。

如收费，请考虑掏钱 or 自行解决。

1.18 其他 3

频道禁言怎么办？有问题看能不能发工单，或于公共群询问相关情况，信息请自行鉴别。

1.19 福利/特色

对 1.5 的补充。

这一部分其实应该放在机场选择那一小节一起写的，不过我一开始也忘了这一部分所以就不想在加了。很多机场提供了如流媒体账号，收费代理的下载，Office365 账号，飞机杯??? 等第三方的服务。//可看毒药的博客，有详情。有些则基于自家的服务，进行了个性化的定制，如 Dler 自己写规则，还提供了定制的客户端；YoYu 则提供了很全面的订阅筛选设置项。其他待补充。

1.20 其他 4

本文档的第二部分是代理软件综述；第三部分是代理软件的下载与使用；第四部分是报障的相关；第五部分是拓展，主要是概念解释。

暂时就这样吧，开始你的翻墙大业吧。Enjoy！

2 代理软件综述

代理软件综述，这段只是为了部分有需求的用户快速了解相关知识

2.1 常用/见语解释

Quantumult 俗称圈/quan

Quantumult X 俗称 quanX。和 quan 同一作者。最早是作者出于个人兴趣，与 quan 有不少差异。可通过 TF 通道申请。

Shadowrocket 俗称小火箭/部分输入法快捷关联为小火煎。Pharos Pro/Pharos，俗称小水滴/水滴/法老？跨平台支持 iOS/Android（对应前后顺序）。

Kitsunebi 狐火，跨平台支持 iOS/Android。

Surfboard 冲浪板

CFW Clash for windows

V2RayN/V2RayNG 是同一作者

HMBSbige是近来较为活跃的 SSR 客户端开发者，目前 Windows 版界面已有较大改动，也有意向接手 Android 版。

SSD 的作者，拉黑了大部分的国产系统，但有人提供了解除限制的版本。SSD 最新版可于 issue 进行下载。

aff/affman：推广链接和邀请别人进行注册（支付）从而获利的人。

tf/TF：TestFlight 是苹果旗下的应用测试平台，能帮助开发者邀请用户对 App 进行测试，方便开发者更好地改进和完善 App。

bot：bot 是英文单词 robot 的简写，略语。而 robot 的意思就是：机器人，自动机。因此 bot 是基于我们设定好的程序就开始自动工作。对很多人来说，bot 是不会污染聊天界面的一个交流工具。

VPN：现在国人语境下的 VPN 就是翻墙软件的意思，不要和原始语义混为一谈。

UDP：部分游戏或通信软件在进行通话的时候需要 UDP 转发。

tg/TG：Telegram 是一个跨平台的即时通信软件，提供友好的即时交流，多平台自动同步，可连接预览，有强大的 bot 功能，需翻墙才能使用。配合关于 bot 的解释，默认情况下，不要随意私聊他人，私聊他人请事先征得同意或通过 bot 沟通。

被打/D：即 DDOS 攻击，是一种网络攻击手法，其目的在于使目标计算机的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。

被 C/CC 了：CC 攻击（Challenge Collapsar）是 DDOS（分布式拒绝服务）的一种，攻击者借助代理服务器生成指向受害主机的合法请求，实现 DDOS 和伪装就叫 CC。

cf/CF：Cloudflare 是一间总部位于旧金山的美国跨国 IT 企业，以向客户提供基于反向代理的内容分发网络（Content Delivery Network, CDN）及分布式域名解析服务（Distributed Domain Name Server）为主要业务。Cloudflare 可以帮助受保护站点抵御包拒绝服务攻击等网络攻击，确保该网站长期在线，同时提升网站的性能、加载速度以改善访客体验。//摘自维基

托管：简单地说就是机场帮你搞好了一切，你只需要导入，不需要自己维护节点的排列，规则的编写。surge/clash 采用的是托管策略，当然，这些软件也提供了相应的手动设置选项。。

策略，这个复杂，你需要第四部分的解释。简单来说，策略是决定一个网络请求是如何工作的/直连/代理/拒绝。

为什么有这么多叫 Clash 的？

Clash 为 Go 语言编写的命令行使用程序，基于文本配置，没有图形界面。对一些人来说操作不够方便。也因此出现了很多第三方的图形界面，大大方便了使用。如 CFW,Clashx,clashA 等。顺便，Clash 也有路由器版本 KoolClash，请需要折腾的用户自行发掘。

2.2 快速入门节点导入

快速版入门节点导入，除了某些机场提供的定制版客户端，其他的机场提供的代理软件支持都是基于第三方客户端。因此你需要使用一些方法导入你的节点信息

常用的如链接导入/扫码/订阅

早期的时候，服务器的信息需要手动填写。后来有人觉得不方便就有了链接导入，有人觉得链接还不够方便就搞了二维码扫描，方便手机端录入。因此，在 win 版的 SS/SSR 客户端你还可以见到这两种添加方式和分享方式。

但针对多节点的导入和节点信息的更改，这些方式还是略显的麻烦，于是就有了订阅导入。你只需要复制一个链接，导入支持的软件中就可以方便的一次性导入多节点和管理更新。也因此，这个订阅链接特别重要，千万不要分享/泄露给别人。影响小的只是损失流量，影响大的会导致账户被删封。一般，这个条款每个机场都会有。

那么问题来了，我从哪里获得订阅链接呢？

一般在你购买后，在网站的个人中心可以找到你激活的服务，点开，里面会有很多节点信息。现在很多机场还保留了链接/二维码导入。你可以根据你的需要，导入节点或者采用订阅的方式。

具体各订阅方式和支持的软件请参考此图。

2.3 废话，概述协议和软件状况

以下废话，建议别看

最常见，支持度最好的是 SSR 订阅，SIP002 也还好，VMess 虽然乱，不过有办法解决。SSD 搞出了自定义的 SSD（订阅后支持导入到原版客户端/通常情况下这些节点都需要你提前下载安装好 obfs 插件，要不无法使用。。。）。以 Surge 为首的软件搞出了托管。但有趣的是 Surge 每个大版本对前一个版本的托管支持程度都不一致，Surge3 支持 Surge2 的，不过大多

数机场还是独立出来，建议你按名字来，要不出了错别怪别人。Surge4 不支持 Surge2，目前来看是支持 3 的。。。

以 SS 官方社区为代表的开发的软件，到目前为止还不不支持订阅。而且 SS 的功能拓展是基于插件的，各软件对插件的支持各有不同。SS 要玩插件还是自建吧。

V2Ray 是非常全面的网络工具，VMess 是其自有协议。目前说大部分提供 v2 的机场基本只提供 VMess 协议支持，没有提供完整的 V2Ray 支持。V2Ray 的操作自由度度更高，功能也强大，基于文本的配置，适合个人使用。

其他的代理工具目前还有些小众，诸如 Brook，Trojan 等。但也有机场提供对 Trojan 的支持（据我所知）。

我想说的是对用户来说，决定使用体验的其实是节点的质量而不是协议，所以你没必要那么在乎协议，你又不懂不是，除非你对某人/软件/名称情有独钟；同样重要的是你使用的客户端，这才是你见的最多的，其实我倒是希望你见的少一点，存在感别那么强。同理还有机场官网。流行的客户端支持了主流的支持格式，又反过来影响用户的选择。

所以，除了对协议有要求的，考虑机场支持什么协议并不重要。同样的，机场的线路是怎么走，IPLC 是哪种专线，对你来说也并不重要。企图在群里得到详尽细致的解答是不可能的，如果你真的想了解，其实已经有很多科普了，你确定你搜过并且看懂了吗？在群组聊天中，除了技术讨论，这些概念只是语气词出现而已。第一部分的选购已经基本够应付了。你有纠结到底的决心，考虑自行解决/花钱。

特色解释

VMess 订阅格式很有特色。通常我认为 V2RayN 的订阅格式是 VMess 的基础。因为其他支持 VMess 订阅的大都可以通过对 V2RayN 订阅的转换而得到。

quan/小火箭/pharos pro 的的 VMess 都是是自有格式，有的支持导入不支持导出，有的支持导出只能给自己用。。。不建议手动添加和导出，请使用机场的订阅链接进行操作。

而 quan X 取消了对 VMess 的支持。

一样会令人理解不清的概念，VMess 和 V2Ray 是什么关系？

VMess 是其自有协议，在这个层面上看，可以认为 VMess 和 Shadowsocks 协议是等价的。但 V2Ray 是一个工具集合，支持如多协议支持，可定制

化路由等特性，与 SS 还是有所不同的。TG 群组常说的支持 V2/V2Ray，基本是代表 VMess。这一点一定要记住，不要混为一谈。基于 V2Ray core 核心的客户端支持 V2Ray 的所有功能。如 kit/V2RayNG。而 quan 等只支持 VMess 这个格式，并未提供完整的 V2Ray 支持。而 V2RayN/V2RayN/V2RayNG, Kitsunebi 都是完整的 V2Ray 实现，这也是说这些软件有高级的玩法。不过那是你自行折腾得了。

Trojan：模仿了互联网上最常见的 HTTPS 协议，以诱骗 gfw 认为它就是 HTTPS，从而不被识别。trojan 工作在 443 端口，并且处理来自外界的 HTTPS 请求，如果是合法的 trojan 请求，那么为该请求提供服务，否则将该流量转交给 web 服务器 Nginx，由 Nginx 为其提供服务。基于这个工作过程可以知道，trojan 的一切表现均与 Nginx 一致，不会引入额外特征，从而达到无法识别的效果。当然，为了防止恶意探测，我们需要将 80 端口的流量全部重定向到 443 端口，并且服务器只暴露 80 和 443 端口，这样可以使得服务器与常见的 Web 服务器表现一致。这部分 Trojan 来自自建梯子教程 –Trojan 版本

2.4 简单的协议支持概况

以上很罗嗦，下面是简短的协议是支持情况，具体到软件的支持请以软件为准。

SSR：自家的协议，连体的混淆

SS：自家的协议，外挂的混淆

VMess：自家的协议，多种请求方式，完善的混淆（VMess 的伪装一般不叫混淆？）

Trojan：模仿了互联网上最常见的 HTTPS 协议，以诱骗 gfw 认为它就是 HTTPS，从而不被识别。

然后对表格中协议的解释：

SIP002 是 SS 的一种 URL 支持标准，可用于订阅，支持 obfs 混淆。因此订阅有带/不带 obfs 的区别。有的软件只支持不带混淆的，如 kit。Pharos 支持带 obfs 的。

Clash 基于 SS-GO/V2Ray，支持 obfs。

SSD：支持 obfs

SSD/SS 的 obfs 以插件的形式提供，安卓版可于 play 商店下载，也可手动在 GitHub 下载。win 版 SSD 自带 obfs，SS 请自行 GitHub

surge 托管支持 obfs

quan/小火箭支持 obfs

一切以机场服务为准。我也提供了图，展示常见的软件及下载方式。

2.5 iOS 平台代理软件简单介绍

这一部分是很轻松的闲聊

具体协议支持轻查看此图我也提供了图，展示常见的软件及下载方式。//我还没学会插图片，请手动外挂。部分在第二部分有链接，全部链接在第三部分都有提供。

下面简单介绍一下代理工具的特点：

iOS 平台的代理工具质量都非常高，而且支持完善，安卓好羡慕。//价格来自聪聪大佬的网页SS/SSR 简介

quan 和小火箭往往被一起讨论，支持都非常全面，是代理工具界的翘楚。差别是 quan 的设置细项更多一些。都支持节点订阅，规则订阅。价格为 4.99/2.99 美元

pharos pro 是新出的代理应用,支持协议非常广泛,SSR/SIP002/VMess/Torjan。内置代理规则，操作简单，易上手。价格为 2.99 美元.

surge 是策略组开创者，它只支持原版 SS 和 obfs 混淆，部分场景下可用于网络流量的抓包与分析，功能远超一般的代理工具（价格也是）。免费 + 内购 49.99 美元.

kit 是完整的 V2Ray 支持。支持 VMess 订阅，支持 SIP002 订阅，支持规则订阅。售价 4.99 美元.

quanx 是 quan 作者的新作，quanx 和 quan 比，一个大的改变时去掉了对 VMess 格式的支持。似乎是转为了支持了 SS+V2Ray 插件。因国区苹果商店下架了 VPN 类应用。如需使用上述提到的应用请自行搜索资料建立美区账号支付购买。或者机场由提供购买支持的请与机场联系，按照相应的规定。或者自行淘宝进行购买，这大概最方便了。请尽量支持正版。真的好用，就没什么多提的了。

2.6 Android 平台代理软件简单介绍

Android 上其实好的代理工具不多，//分应用是安卓的一个特色功能，可自行选择代理/直连，强烈推荐使用。而 iOS 则基于规则。

尤其是 SSR 系软件在软件作者停止开发后，版本众多却改进不大，更新也少。近来倒是出了一些好转的迹象，有人在更新了。有些机场如 rixCloud 提供了自修改版本，另一些则有换壳版的账户登录型定制版客户端，如 Nex。具体的参考我的各平台软件下载方式或聪聪大佬的博客，他的更全面。聪聪大佬的网页SS/SSR 简介

其实，近来也有好转。Maying 是同名的机场的一位用户开发的，对原版略有改进，主要是添加了 ACL4SSR 的规则。目前已停更，可于谷歌商店下载。同样，近来再 win 版 SSR 的维护与开发上表现出色的 HMBSbige 同样也有意开发 Android 版 SSR。

原版的 SS 不支持订阅，在订阅时代显得格格不入。有基于原版 SS 开发的 SSD 支持订阅，支持与原版 SS 互通数据。可惜的是作者对多数国产 ROM 的态度是要么拉黑，要么在拉黑的路上。不过有解除限制的版本，请考虑自行下载。不少网站倒是基于它定制了自己的客户端，方便账号直接登录，免去导入订阅的麻烦。比如 Dler 提供的 SSD-Android 0.0.6。

不过最近倒是有新的作品表现还不错，或者说看到了一些希望。

Pharos 支持 SSR/SIP002 订阅。支持扫码。使用内置规则代理。目前安卓上 SSR 协议支持表现的最好，极大的减少了断流。//代理以内置规则为准，请考虑提交应用。目前处于开发早期，操作简单。但有一些注意事项：订阅链接导入后，点击获取，默认是无提示的。可以在订阅服务器列表查看。支持扫码，网站没直接提供的话可尝试使用 win 版 SS/SSR 以二维码格式分享。目前最大的麻烦是切换节点较为麻烦，建议以扫码的方式添加常用的节点。或选择更稳定的机场服务，即不怎么需要切换的。更新订阅在订阅服务器里查看，选择你的订阅，点击，在右上角有标志。建议机场服务稳定且支持 SSR 的用户进行尝试。目前的代理是以内置应用代理规则，若你使用的软件未能代理，请加入群组，寻找提供包名的办法。或商讨新的解决方案。目前安卓免费，请考虑 github 点赞。

surfboard：兼容 surge2（请提供更多信息），是安卓少有的支持托管的软件，内置分应用。使用很方便。目前更新频繁。支持 SS 的机场大多支持 surfboard。目前 ping 功能貌似有一点毛病。

SSD 即 SS 加上了订阅功能。不过却不是 SIP002，订阅后的配置文件可直接导入原版 SS，部分节点需要 obfs 混淆，请于谷歌商店/GitHub 下载。

kit 支持 SIP002，VMess。支持订阅规则（如神机规则）支持分应用。

V2Rayng 支持 SIP002/VMess。支持分应用。操作简单。

clashA 支持 clash 托管。设置项不多。可于TG 群组TG 群组获得最新测试版，请遵守相应的群规，仔细阅读置顶。

outline 支持原版 SS，不支持混淆，不支持扫码。

2.7 Windows 平台代理软件简单介绍

SS-Win 由官方社区维护，支持扫码，不支持订阅。可由 SSD 订阅后分享导入或下载机场提供的配置文件，如 rix。

Clash （CFW）是易用的 clash，使用托管。可在软件内启用 uwp 应用的代理。使用省心。强烈推荐。目前有修改版的ClashR。

SSD 如安卓

outline 有别于系统代理，是真全局代理。

SSR 的情况有些复杂，原版的 SSR 在作者退出后停止维护。大量第三方出现。情况和安卓的情况差不多，请参考。HMBSbige 开发的 win 版使用体验很不错。

SSTap 已停止维护，可以订阅 SSR，也适合打游戏。不过近来的 netch 表现也不错，快速开发中。

2.8 macOS 平台代理软件简单介绍

说实在我不熟悉，就和路由器一样，所以我没提路由器，我没需求，我喜欢自由的切换节点。

surge 和 iOS 一样的功能。另有办法支持 SSR。自行发掘。

另有 ShadowsocksX-NG 支持 SIP002

ShadowsocksX-NG-R8 支持 SSR 订阅

另有大量其他客户端，请自行了解。

2.9 一个尝试：解释协议与混淆–不要脸版

最后的最后，简单的提一下协议和混淆。这一部分我基本晕着写的。

我先举个例子，这例子不一定合适。

我们以视频格式为例，为方便叙述，我选择了 MKV 格式。我先假设大家都尝试过本地播放过这个格式，那如果你曾留意，会发现很多时候有地方标识未 AVC1，AAC 这两个字符。

简单的做一下解释：AVC1 是你所观看视频的图像（视频轨）的格式，编码标准是 H264。以视频轨举例。

AAC 是音频轨的编码格式，那 MKV 是装载他们的容器。看视频的话你不可能只能看图像轨/只能听音频轨。这一部分理解没问题吧。而播放器是载入这个 MKV，分轨，然后由对应的解码器识别 AVC1/AAC，进行播放。

这也是我觉得与代理服务器协议有关的地方。虽然不一定准确就是了。

你原始的数据流–协议编码–加密–混淆

原始的数据流–H264 编码–加密？–封装

简单的解释一下：你的网络流量经过 SS 协议定义的方式进行编码–采用协议支持的方式进行加密–然后得到一个 A 数据包，这个数据包会被 gfw 识别为未知流量，正常情况下，gfw 会选择放行。这是第一阶段。

就好像是一个采样的数据流经 H264（伪）编码得到 AVC1（伪），在本地播放器进行播放时，我们假定 AVC1（伪）会被识别成 AVC1 进行播放。（此处的单 AVC1 的情况可考虑删除音频轨，或说我为啥不选一个 flac 格式呢，好像是缺一个步骤。。。）

所以协议和加密的可以理解为得到一个无法识别的数据包，然后进行放行。

混淆的出现最早是为了解决部分 ISP 对于非 HTTP 和 TLS 的未知流量，进行的降速限制。

这一部分可以用 MKV 封装 AVC1 来解释。我们把 AVC1（伪）也套一个 MKV 的壳。让运营商以为这是很正经的流量，进而解决限速问题。而这壳有多种套法，也就有多种混淆的实现，有些协议只支持特定的混淆。

进一步的发展，某些协议配合混淆在 gfw 处可实现较好的抗代理流量识别的效果。

需要说明的是不同的混淆对协议的伪装是不一样的，例如 http___simple 是提供一种强特征，试图欺骗 GFW 的协议检测。一般情况下，你使用机场的服务的时候并不需要关心这一点。个人请自行琢磨。

3 代理软件的下载与使用

以下大部分下载方式来自聪聪-SS/SSR 简介 另外推荐聪聪博客的其他两篇博文：Telegram 知识,Telegram 群组、频道、机器人 - 汇总分享，帮你

快速入门 Telegram。

另外，我并没有对我所列的所有软件的教程进行整理，一部分是认为不必要，一部分是没有好的，最大的原因是因为懒和没动力，这一部分确实不好处理。//头昏眼花，复制出错。

请优先参考你的机场提供的教程，订阅链接类型，推荐软件等。

如果都没有，请自行谷歌，看个十几二十篇了解个大概，这样即使你还不会，问的时候也好处理一些。

3.1 Android 客户端

3.1.1 SS

下载：Shadowsocks 影梭 Shadowsocks 影梭 Google Play obfs 插件 obfs Google Play 使用：自己努力

3.1.2 SSR

下载：text text text text HMBSbige 使用: 无

3.1.3 Pharos

下载：Pharos 使用：参考本文第二部分

3.1.4 Kitsunebi

下载：kitsunebi-android 使用：使用说明 规则导入

3.1.5 Surfboard

下载：Surfboard 使用：使用

3.1.6 V2RayNG

下载：GitHub Play Store 使用：无

3.1.7 ClashA

下载：GitHub 使用：暂无

3.1.8 Igniter

下载：Igniter 使用：

3.1.9 SSD

下载：SSD 使用：

3.1.10 Outline

下载：Outline 使用：

3.2 iOS 客户端

3.2.1 Quantumult

下载：Quantumult 使用：

3.2.2 Shadowrocket

下载：Shadowrocket 使用：

3.2.3 Pharos Pro

下载：Pharos Pro 使用：

3.2.4 Surge

下载：Surge 使用：

3.2.5 Kitsunebi

下载：kitsunebi 使用：

3.2.6 墙洞/Ihie1

下载：主页 使用：提供了多软件的导入说明

3.2.7 神机规则

下载：主页 使用：提供多软件的导入说明

3.3 Windows 客户端

3.3.1 Clash For Windows

下载：CFW 使用：F 大 用户提供

3.3.2 SS

下载：Shadowsocks 使用：无

3.3.3 SSR

下载：HMBSbige 修改版 breakwa11 破娃最后一版 SSRR Anankke 使用：无

3.3.4 SSD

下载：SSD 使用：

3.3.5 V2RayN

下载：V2RayN 使用：无

3.3.6 Netch

下载：Netch 使用：Netch 说明文档

3.3.7 SSTap

下载：SSTap 使用：

3.3.8 Outline

下载：GitHub 使用：无

3.4 macOS 客户端的选择和使用教程

3.4.1 ClashX

下载：GitHub 使用：

3.4.2 Surge for Mac

下载：官网 使用：

3.4.3 ShadowsocksX-NG

下载：GitHub 使用：

3.4.4 ShadowsocksX-NG-R8

下载：GitHub 使用：

3.4.5 electron-SSR

下载：GitHub 使用：

3.4.6 Outline

下载：GitHub 使用：

3.5 游戏篇

3.5.1 PC

SSTap Netch

3.5.2 主机

PS4 XBOX

3.5.3 手机

4 错误自查/常见/报障

4.1 概述及提醒

请注意，有礼节，有逻辑地表达你的问题，语气很重要，不要去找别人认保姆。

提问题，干脆直接，具体有细节，有逻辑，千万别只说一句我有问题/在吗，我有麻烦了/我怎么上不了网了/我啥都没干啊诸如此类的糟糕提问。而

同时，理解回答和提问是一体的，你需要理顺回答者的逻辑。千万记得：有建议（尤其是来自群组管理者/多数相同的意见），请一定做出尝试，然后及时反馈。细节注意在第一章就有提到，请注意打码个人信息/IP/服务器信息等。

同时，需要说明一下，这个部分我确实没有好的思路，因为出错及解决错误的花样和方式太多了，而我个人能力实在有限，再加上有些问题其实是接近玄学，有些需要远程支援，实在难以尽数，故在此仅是提供几条思路以供参考。这部分有部分内容重复。// 碰到的奇葩问题太多了。。。。

另一个原因是，大部分的提问没有重点，没有逻辑，故而做一个好像也不能说模板的东西吧，提供参阅样例。注意：模板不能涵盖多少问题。

其次，机场提供的是商品和有限的附加支持，指望事无巨细的解决你的一切烦恼简直是开玩笑。但你基本的也是可以解决的，请遵循网站的，群组的提示选择群组提问/工单支持/远程技术支持，或考虑付费快速解决问题。

4.2 自查

本地自查是以下多项操作的基础，以条款的方式列出。

非代理情况下，检查本地网络的连通性，包括但不限于访问国内网址，使用 speedtest 测试本地连接的速度。//是否是正常波动？挖水管把光纤挖断了?。。

代理情况下，如是初次使用，请检查代理软件的设置是否有误，如代理模式/是否开启系统代理/系统代理是否正常工作/SOCKS5 代理是否正常工作/PAC 设置是否正确/是否开启（或关闭负载均衡）/是否选中切换是断开全部连接/切换全局查看是否可以使用/DNS 设置等，打开我第五部分提到查 IP 的网站，打开，看数据是否正确，进行 speedtest 测速，进行同地域，不同地域的对比测试，并检查同网络下其他设备是否正常；

如是先前已有代理，请检查是否已经正确关闭，可于（win10）设置–网络设置–代理，看到你现在启用的代理服务器，如信息有误，请考虑清除。常见 socks 端口如下：SS/SSR:127.0.0.1 1080;Clash:127.0.0.1:7891 mac 版自行查找

4.3 初次导入，无法使用

初次使用，建议在官网多看看，没啥事可以挨着点一遍。我还是优先推荐以机场官网的信息为准。

如你导入连接出错，请查看网站提示重新导入 //我的情况，win 版 SSR 的 PAC 和订阅更新都来得蛮慢的，推荐首先选择不通过代理，如无法更新，请于群组进行询问。如已有节点，可尝试，全局，通过代理更新。

如你正确获得了节点信息，已有自查部分全部未正常设置/已按照网站提示进行设置，请咨询群组/提工单。一般来说，我建议你再看一次。

4.4 单节点报错

如果在使用中有单个/少量节点提示有误，如超时/反应迟钝，切换即恢复。我的建议是，半小时/自定义时间再测一次，若情况依然如此，请考虑报修。保修请遵守网站的设定：工单，群组，bot 等。报修时请提供：

地区

宽带

平台

客户端

模式

节点

进行同地域，不同地域的对比测试，记得打码，使用 IP 查询和 speedtest 等。

4.5 全节点报错

一般情况下，极少会出现，请优先进行本地自检。

然后参照单节点报错，使用相应的渠道提供对应的信息。

4.6 群组询问与工单报障

这是常见的两种报障和获取建议的方式。请参照你的具体情况，提供相应的信息，在得到反馈后建议尝试。

群组询问请礼貌，直接，有逻辑的表达你的问题，展示相关数据；如你实在不会，请采用描述性无感情色彩的语气进行全程叙述（包括自救）。

工单：因为非即时性应答，你可更有时间对情况进行梳理和描述。注意耐心，相关细则，可于群组进行询问。若无相关群组，可于毒药群类公共群进行询问，请不要泄露信息。

4.7 特殊时期的注意事项

我国自有国情在，若碰到相应的会议/节日。不可避免的，相当一部分人的体验会收到影响，我建议你不要急着在群组抱怨，不要急着在群组嚷嚷。因为这一般是你自己造成的，你付出的成本，你大概什么体验，自己要有数。别把预期放的太高。但是呢，一般机场都会有相应的应对措施，如开放专线/过期补偿等。

4.8 浏览器报错

这个最常见也最不好说。我也不过是说如切换模式，查找错误代码，节点对比这样，具体情况具体回答。如遇到单一/少量节点报错/无法使用

5 拓展部分

5.1 IP 库/查 IP/原生 IP/购物

5.1.1 IP 库

IP 库：IP 地址与物理地址的对照数据库 IP 库需要不断进行动态更新，因此准确和覆盖不可兼得，只能取个平衡。目前市面上暂没有公认最优的一个 IP 库，较好的解决方案是融合各 IP 库做取舍。国内比较好 IP 库是 IPIP；国外则是 MaxMind；因为国内 IP • 情况较复杂 MaxMind 的国外 IPIP 较准确，国内则表现不如 IPIP；目前 IPIP 的国外数据和准确度也在迅速提升中。以下三篇文章是关于 IP 的使用常见的问题与解答。

IP 库之手机基站数据篇

IP 库之中国特色第三方出口篇

IP 库之默认就开启云加速的某些浏览器篇

5.1.2 查 IP

我推荐以下两个网址来查看本地和代理服务器的 IP 主要作用是方便在出现本地连接有误的话进行的自查的步骤之一。

Skk

ip111

注意：在你提交/分享的时候，对自己和服务器的 IP 打码。

5.1.3 落地

即你访问目的所识别的 IP 归属：家宽，商宽，IDC 等。

5.1.4 原生 IP/本土 IP

原生 IP/本土 IP：是指 VPS 所被分配到的 IP 的注册地址和 VPS 所在的国家/地区一致的 IP。

广播 IP：VPS 所被分配的 IP 的归属地，不符合该 VPS 所在的地理位置。即，这是从另一个国家/地区广播过来的 IP。

IP 地理位置为什么重要？DNS 解锁又是怎么一回事？

一切都基本可以认为是地区限制的原因。原生 IP 一般不用于公有云计算服务或 IP 声誉好，一般能够用来解锁 Netflix、HBO、Hulu 以及其它有限制的流媒体服务。一个极好的例子 Spotify 的音乐是分区的。同时，很多海外的购物网站也会有锁 IP 的行为，限定本国家/地区的 IP 接入，这个比流媒体的解锁更加麻烦，让不少机场十分难办。毒药笔记

另外提一点，因为谷歌神奇 IP 库的关系，有可能出现你选择美国节点，而你的 YouTube 确实显示的德国区的内容。另一个常见的是谷歌会把部分阿里云的 IP 识别成美国的 IP，进而可以解锁 YouTube Premium/Music。// 新加坡 //需要修改，这里我不会。

而谷歌因自身的原因在很多地区并没有开放 YouTube Premium 等服务，如你需要，请于机场的群组进行询问。

流媒体解锁：很多流媒体服务平台如 Netflix 会出于版权原因而限制一些特定 IP 的访问。一般来说网络运营商（如 HKT）自己持有的 IP，比如商宽、家宽，极少被屏蔽，因为这些 IP 大多是流媒体服务商的目标客户在使用。家宽 IP 被屏蔽的几率是最低的，很多 IS 的家宽都是动态 IP 的，很难精准封杀。固定 IP 的商宽其次。这些流媒体服务商也怕误杀导致投诉，比如 GCP 的 IP 段被投诉之后又可以看 Netflix 了。IDC 商家所持有的 IP 一般会被屏蔽，越大越有名的 IDC 持有的 IP 被屏蔽的几率越高。很多 IDC 会租用运营商的 I 从而绕过此类封杀，但是这种方式并不是万无一失的，翻车案例比较多我就不再一一例举了。所以除非是商宽、家宽，其他所谓的“原生 IP 解锁流媒体”都是有几率翻车的。//摘抄自毒药笔记

5.2 中转/专线/IPLC/GFW/公网/QoS/SLA/CN2，163

5.2.1 中转/中继/BGP

中转：将数据从一个服务器重定向到另外一个服务器。

BGP：BGP 在机场的语境下通常是一个 IP 在多个运营商的网络中均为直连，不经过第三运营商，利用 iptables 或相关软件通过将去海外 VPS 的流量加一层国内转发。所以，BGP 是中转的一种。BGP 中转服务器到海外流量的转发可以通过公网，内网等途径。

5.2.2 IPLC/专线

专线：互连两点之间的通信，即点对点通信，用内网业务和公网业务来区分。

目前所见的机场用的“专线”基本都是以下几种：

公网 Tunnel 转发占了大概 80

阿里经典内网/云企业网占了大概 15

其他 IPLC

CN2 专线：CN2 专线业务是中国电信 CN2 Global Internet AcceSS，由某些卖北美 GIA CN2 的国人商家提出，16 年左右 -> CeRaNetworks（CN2 专线），17 年安畅 -> CDIA （China Direct Internet AcceSS），从而不少人认为这种是真专线，不过 GFW。实则其实只是商家为了宣传而打出来的噱头，即使用 CN2 GIA 一样会在国内骨干网爆炸的时候无法正常使用。当然啦，由于 GFW 都是部署在骨干网出口的，因此自然而然的走公网的业务必定是过墙的，不存在不过墙的 CN2 专线业务。

IEPL 和 MPLS VPN 以及 IPLC 在一定程度上他们做的事情都是差不多的，因此合并在一起。

IPLC/IEPL: IPLC 的概念是用于互连两点之间的通信，即点对点通信。深港 IPLC 的意思是深圳到香港点对点传输而不经过公网，是完全的内网。目前阿里云经典内网/云企业网就是这种，在卸载阿里云盾后是可以被认为是真正意义上的专线。这种专线因为没有走公网因此完全不过墙，你传输什么 GFW 都是不会知道的。

还有一种比较特殊的情况，有一种公网 Tunnel 也是不过墙的，由于 GFW 部署在运营商的出口处，因为国内到国内是没有 GFW 存在的。因此某些机场使用了如下结构构造无墙专线：

徐州 VPS -> 上海阿里云 -> 阿里经典内网 -> 香港阿里云 -> HKT

而这种走法避开了部署在运营商出口的 GFW 而且因为目前国内运营商针对 IDC 带宽是很小的 QoS，HKT 对港内也是不限速的，因此也大大改善了连接速度。这种做法的确是不过墙的，并且因为很多 Tier 2 IDC 的审查并不如阿里云审查那么重，因此也被不少人选择。

总结一下，目前基于公网的业务例如 GIA CN2，BBTEC，9929 均是会有 GFW 的，不仅有被墙风险还会有 QoS 的问题。而目前性价比较高的 IPLC 是阿里云经典网/云企业网搞出来的那套东西，摘自 saber 的万事屋

5.3 QoS/SLA/CN2

5.3.1 QoS

QoS：服务质量（Quality of Service，缩写 QoS）是一个术语，在分组交换网络领域中指网络满足给定业务合同的概率；或在许多情况下，非正式地指分组在网络中两点间通过的概率。QoS 是一种控制机制，它提供了针对不同用户或者不同数据流采用相应不同的优先级，或者是根据应用程序的要求，保证数据流的性能达到一定的水准。QoS 的保证对于容量有限的网络来说是十分重要的，特别是对于流多媒体应用，例如 VoIP 和 IPTV 等，因为这些应用常常需要固定的传输率，对延时也比较敏感。//来自维基百科

在日常使用的语境下，大致是指你的网络服务质量

5.3.2 SLA

流量约定（SLA, Service Level Agreement 服务等级协议）给数据流设定优先级，以此在网络 / 协议层面上，根据相互商定的尺度，设定有保障的性能、通过量、延迟等界限。一些特定形式的网络数据流需要定义服务质量，例如：多媒体流要求有保障通过量。//来自维基百科

5.3.3 163 与 CN2

普通 163: 就是电信用户最经常遇到的电信线路，等级最低，省级/出国/国际骨干节点都以 202.97 开头，全程没有 59.43 开头的 CN2 节点。在出国线路上表现为拥堵，丢包率高。

CN2 GT: CN2 里属于 Global Transit 的产品 (又名 GIS-Global Internet Service)，在 CN2 里等级低，省级/出国节点为 202.97 开头，国际骨干节点

有 2～4 个 59.43 开头的 CN2 节点。在出国线路上拥堵程度一般，相对于 163 骨干网的稍强，相比 CN2 GIA，性价比也较高。

CN2 GIA: CN2 里属于 Global Internet AcceSS 的产品，等级最高，省级/出国/国际骨干节点都以 59.43 开头，全程没有 202.97 开头的节点。在出国线路上表现最好，很少拥堵，理论上速度最快最稳定，当然，价格也相对 CN2 GT 偏高。

CN2 VPS 是否一定比普通 163 承载网络的 VPS 更快呢？

CN2 决定了网络质量会优于普通 163 承载网络，但也不一定，除了承载网络之外，机房的地理位置也很重要。

单向 CN2 与双向 CN2

CN2 除了线路分为两种类型，购买时，还得注意 CN2 是双向还是单向。所为双向，顾名思义，去程的路由节点和回程的路由节点，都使用了 CN2 的承载网络。而单向 CN2，一般都是去程 CN2，回程普通电信线路，在速度上，会略逊于双向 CN2。

以上 CN2，163 部分来自CN2 的那些事-CN2 线路与 VPS 服务商介绍

这个是国内主流网络运营商国际连接线路简谈

补充：

以上的说明不是为了让你追问机场的具体线路到底是个啥情况。作为交付式的服务，最重要的是服务的可用性，其他的真不太重要。

通信端口（英语：port），又称为连接端口、端口、协议端口（protocol port）在计算机网络中是一种经由软件创建的服务，在一个计算机操作系统中扮演通信的端点（endpoint）。每个通信端口都会与主机的 IP 地址及通信协议关联。通信端口以 16 比特数字来表示，这被称为通信端口编号。常见端口如 443-HTTPS/80-HTTP 端口，这些是固定端口，而机场的部分端口为非常见端口，比如 6353？

部分机场以常见端口提供服务，再某些公司内网且限制端口的情况下，可取的较好的效果。

5.3.4 宽带服务提供商与 VPS 商家

宽带服务提供商与 VPS 商家

宽带服务由本国的运营商提供，VPS 商家都是购买的本国运营商的带宽进行本国交互/跨国交互。而各种其他服务的提供情况则根据 VPS 自身持有的 IP 决定。

具体可参考：机场常用线路科普 毒药笔记

5.4 DNS 与 GFW

5.4.1 DNS 污染

DNS 污染，这是访问中不可避免的一部分，现在各大客户端基本都有远程解析的机制，确保你可以正常访问外网，但本地路由的处理就大有不同了。一般情况下，我们默认使用的是运营商提供的 DNS，但运营商也是分地区的，不同地区运营商政策不一样。某些可能就给你搞了劫持，这也是最常见的。如你遇到此类情况，包括但不限于/待添加/，你可考虑更换 DNS，参考文章是 skk 的简介。现在有些工具也置了避免 DNS 污染的功能，如 Clash。其他的你可以考虑设定 smartDNS，进行防污染。//DNS 也是 GFW 常用的手段。其他部分，自行维基。也可参考浅谈在代理环境中的 DNS 解析行为 | Sukka's Blog及关联文章。

5.4.2 GFW

请自行维基

和参考深入理解 GFW：内部结构，不过这是 10 年的文章。

5.5 分流/PAC/路由表分流/策略/规则/策略组

5.5.1 分流

分流：以往的 VPN 是可以代理各种协议，这使得部分可以正常打开的网站打开缓慢。而到了 SS 协议代理的时代，因为是 socks5 代理（有解释），已经不能像 VPN 一样代理各种网络请求。这也带来了改变的可能。即可通过一定的规则进行流量的分发，从而加快访问速度。

分流的意义，初期是为了解决国内/国外使用同一网络模式访问缓慢的问题，如挂全局访问国内视频网站等。后来，由于不同的客户端提供了多种多样的分流方法，网上也出现了很多人基于相应制作的规则集。现如今很多人所说的分流已经不仅仅是国内直连，国外代理了某种意义上，折腾分流俨然成了技术活和一部分人的技术象征，他们乐此不疲。

socks5：根据 OSI 模型，SOCKS 是会话层的协议，位于表示层与传输层之间。SOCKS 工作在比 HTTP 代理更低的层次，只是单纯传递数据包，

不关心具体协议和用法。

代理的区别/什么是系统代理

简单的说，你只需要知道支持系统代理的应用很少，对个人的应用场景就浏览器或 IDM。

TG 建议手动添加 socks5 代理，这样再系统代理模式切换的时候不受影响。//系统代理失效时，可看 socks5.

然后是直连即浏览器的一切流量或者说请求都不经过代理服务器。

全局即（主要）浏览器的一切流量或者说请求都经过代理服务器。

代理即流量或者说请求都经过代理服务器。实际应用语境下的代理往往指通过某种分流方式进行流量分发后经过代理服务器的方式。

5.5.2 PAC1

PAC：代理自动配置（英语：Proxy auto-config，简称 PAC）是一种网页浏览器技术，用于定义浏览器该如何自动选择适当的代理服务器来访问一个网址。//来自维基

即只针对浏览器起作用。PAC 有其语法格式可以自行编辑，不过对个人来说维护起来成本比较大。现在主要采用的是他人维护好的规则。比如 gfw/gfw-white 等。这在 SS-win/SSR-win 的设置界面都可以看到。

gfw：great fire wall 防火长城，也就是墙。这个也被叫做黑名单，是由社区维护的，收集整理被 gfw 阻断访问的域名，IP。使用此规则时，匹配规则的会走代理。

gfw-white：俗称白名单。名单内容是大陆域名和 IP。使用此规则时，符合规则的会直连，规则外的会走代理。

就其两者进行比较：gfw 的维护由社区进行，在有新域名被墙时不一定会立即收录。（如有发现，请考虑提交）gfw-white 的思路是，大陆域名相对稳定，而跟着墙走不一定及时。此外，某些未被墙的网站或拒绝大陆 IP 的网站因其地理位置和个人直连海外的网络质量的影响，使用代理会相对稳固。对个人来说，gfw 的使用会相对省流量，gfw-white 会消耗相对多一点的流量。对于流媒体服务，推荐白名单模式。个人没什么特别需求，gfw 一般就够了。某些机场的主页拒绝了大陆的访问，若使用 gfw 进行访问，需要在系统代理设置为全局，刷新页面，白名单一般没这种担忧。

5.5.3 路由表分流

路由表分流可参考 SSR-win 上，由 PAC 分流规则和路由分流。路由分流这时需要你在浏览器自行添加 socks5 代理或使用 Proxifier 建立系统代理。浏览器可使用 switchyomega。同样如 win 的 V2RayN 的设置由路由分流。但这里其实不是太详细和准确，如 Android 的 SS/SSR 是基于 ACL 分流，有第三方制作的 ACL，iOS 则有规则分流（略说）。因常见的协议本身并未规定如何分流，均有软件自身实现。

5.5.4 PAC2

针对 win-ssr 客户端的两种方式，PAC 和代理规则。（这与 V2RayN 的有点像，我不知道机制。）

以下内容来自逗比根据地，他的观点是 1.PAC 规则是根据 PAC 文件中的黑白地址名单来判断那些网站走代理。也就是判断流量是否进入客户端。2. 代理规则是根据 IP 判断，按设定的规则来判断进入客户端的流量是直连还是走代理。

这看似有那么点道理，不过我的疑问是为什么为什么要多一步判断？意义何在？

我原本的看法是 PAC–系统代理，分流规则–SOCKS5 代理（浏览器添加插件）

我把问题放在这里，请自行研究。

5.5.5 策略组分流

在此之前先自行了解节点，直连，代理。此处会有 reject（拒绝）规则项。

作用方式和其作用对象合成为一个策略。作用方式包括：proxy，direct，reject 和域名匹配方式，作用对象为网络请求。

此外还有规则一词，意项较多。可指，一条具体的匹配规则，一个规则集（如神机规则，谁有 XX 的规则）一个由策略组成的策略集。//这里我的说法基本是根据 Clash 进行说明的，其他的请自行理解。iOS 有个情景模式，再自动选节点的时候提到过，这里的用法就不同了，简单的说就是连 WiFi 怎么办，连数据怎么办。

策略组由策略构成，策略组可直接应用于策略中的规则或被其他策略组调用。

举例如下：

你发出了一个请求 www.google.com，经规则初步匹配属于 proxy 策略组，按照 proxy 相应的策略。假设你 proxy 关联的是 hk3 节点，则经代理本地流量发往 hk3 节点。

你发出了一个请求 www.iqiyi.com，经规则初步匹配属于 direct 策略组，按照 direct 策略，默认就直接发送到 iqiyi 的服务器了。当然如果你有国内节点则可以将流量发往对应的代理处再发往 iqiyi。

你发出了一个请求 www. 广告.com，经规则初步匹配属于 reject 策略组，按照默认 reject 策略，拒绝此请求。

此外，往往设定的规则还会有所遗漏，此时会有 others 对此请求进行匹配，指定代理/直连。

初步匹配则有多种方法，例如 clash for windows 依赖 GeoIP 库进行请求的判别看是否需要代理。（CFW 也可自定义策略）

同样的，因策略是由规则及其作用对象结合的。所以你可以指定某些域名（作用对象）进行 proxy（操作）。也因此出现了他人定制的策略（有时也称规则/规则集）：对常见的域名规定为代理/直连，对广告，危险网址等进行拒绝请求。

托管：多指机场对你所购买的套餐内的节点和操作进行预先的定义。这样就免去了手动设定规则的麻烦。

策略的有点在哪里呢？当你在浏览器同时打开了 A，B 网页。而 C 服务器对 A 友好，D 服务器对 B 友好，此时 PAC 分流将无法操作。而基于策略可正常使用。此为一处优点。常见应用场景是指定 Netflix 的地区。

再具体一点：

proxy 策略组中，在多节点的情况下你可以依据一定的规则进行节点的选择，如：手动选择 select 延迟测试 url-test 选择延迟低的节点

网络类型 SSid SSID Policy 根据网络类型或路由器名称选择节点或策略组等

而上述所提，可为 Netflix 建立一个 GobalTV 的策略组，在此策略组之内，可以添加你用来看 Netflix 的节点，或选择你当下使用的 proxy 策略。//此处参考自 F 大，我的观点不代表 F 大的观点，请自行阅读链接的文章并理解。关于策略组的理解 by.F 大

5.6 倍率/延迟/自动选节点

5.6.1 倍率

倍率：计算你消耗的流量数值与服务商统计的流量数值之间的比值关系。机场服务常见有两种倍率：普通倍率，最低倍率为 1 倍率；低倍率，有部分节点的倍率低于 1。

举例如下，你使用 0.2 倍率的节点，消耗 1G 流量，则在服务商那里统计为 0.2G。

倍率的意义，倍率与线路质量/用户体验之间的关系

现在机场大致分两种线路类型：直连线路和中转线路。不同的线路类型的流量价格是不同的。大流量甚至是无限流量基本只有在直连线路可以提供，一般使用普通倍率，方便查看和用户理解；中转或是专线的成本较高，在价格不至于夸张的前提下，提供的平均流量是少于直连线路的，而为了保证用户的正常使用和平衡流量价格，因此提供了低倍率节点，方便用户根据自己的需求选择线路。

CDN：内容分发网络（英语：Content Delivery Network 或 Content Distribution Network，缩写：CDN）是指一种透过互联网互相连接的计算机网络系统，利用最靠近每位用户的服务器，更快、更可靠地将音乐、图片、影片、应用程序及其他文件发送给用户，来提供高性能、可扩展性及低成本的网络内容传递给用户。//维基百科

举例：你发起对 YouTube 的访问请求，最终提供资源的的是离你最近的 YouTube 部署的 CDN。

5.6.2 延迟与测速

ping/延迟/测速的意义

常规意义上的 ping 是指向目标主机传出一个 ICMP 的请求回显数据包，并等待接收回显回应数据包。程序会按时间和成功响应的次数估算丢失数据包率（丢包率）和数据包往返时间（网络时延，Round-trip delay time）。//维基

但单纯说延迟，你可以看到测一次延迟，却可以得到好几个数据。举例说明如下：

icmp ping：经典的 ping，在中转的情况下，一般测出的是你到中转服务器的网络时延

tcp ping/http ping：则指发送对应协议的数据包得到的网络时延。一般数值大于 icmp 的值。

如 Clash 的自动测速指定有 url：这个。这个 url 的好处在于全球都有 CDN?，数值相对准确。

下面简单说一下我对测速的理解，测速只是反应当地，当时，某个/些节点的速度状况，然后再这个对同地，同宽带的有较大的借鉴意义，对其他地区的实际参考意义不是太大。但我们仍可以从中找到自己想要的一些数据，例如节点数量，地区分布，连接类型，倍率，某个地区的两个延时参数，基本是这样。当然了，特别普遍的差自然是离得越远越好（非特殊时段，特殊时段另作考量）。自从有了便捷的测速工具，很多人就没事测一下速，一旦有一个节点有了问题，就打算找机场主理论（一部分）或降低对此机场的评价。其实大可不必如此，除了让你一人独享的线路，其他都是共享资源，因人群选择的偏好，不同节点的利用率不同，可供你使用的也许就没那么多。当然了，如果长期如此，那是不能接受的。至于在特殊时期，在你自己选择的机场没那么好的时候，频繁测速反而会让你们整体的体验不断下降。这里也想说，没啥事就别老往香港挤，尤其是排号靠前的。这里要说一下，有人用 YouTube 的码率作为评价的标准，个人感觉没有意义。你 4k 视频所需码率也不高，而切换的相应速度是由节点地区决定的，流畅切换即可。//YouTube 是单线程。

但也不是说你就很被动了，就听之任之了，没那个必要。如果你测试 ping 值过大/timeout，再过几分钟后再测依然如此，你可以遵循第四部分的参考进行提问。

这里推荐一种测速方式。speedtest 测速。在你本地节点出问题的时候，先断代理测本地，在测代理，测同一地区，不同地区，建立对比组。//fast 测的是 Netflix 的状况，不具有普遍意义。

5.6.3 节点选择机制

负载均衡/url-test/fallback/SSID

这些放在一起说，其实严格意义上来讲负载均衡是一种机制，而软件实现的是一种策略。

这都都是自动切换节点的办法，有别于手动切换节点。

负载均衡机制最为常见，有很多类型/延迟/下载速度/错误率等。使用时软件会按照指定的策略，按照某个时间间隔不断地请求访问。// 容易造

成实时连接数超出服务商限制，而且在机场节点稳定的情况下不推荐使用，没有意义，也容易是你不能正确观看到你想看地区的内容。//剩下的简略说

url-test：通过对固定 url 发出请求，通常为 这个，来切换节点

fallback：按照节点顺序选择第一个可用节点

SSID：根据网络类型或路由器名称选择节点或策略组

另外一些造成连接数爆表的如 quan 的测速，也被某些机场禁止，造成越测越慢。

5.7 Netflix/盒子奈飞/土区车/分辨率问题/

与国内不同，许多国外的流媒体服务提供商对软件/系统的 DRM 要求很高。这对习惯性阉割谷歌服务，自立门户的国内手机厂商影响很大。Netfix 的清晰度无法手动调节，在这个前提下和收集 DRM 级别限制的情况下，部分用户播放的清晰度锁死在 540p，更甚者无法于谷歌商店下载对应的软件。

用户可于谷歌 play 下载 drm info 查下 winevide level。

L1 支持高清，720/1080。可于视频详情页面看到 HD 字样/HDR/杜比视界等

L3 支持 540。国内手机一般是，如有需要，请刷国外版 ROM。

此外 root 过的手机一般都是 L3。

手机端具体支持可与 Netflix 搜索 test pattern，播放后，可于右上角看到分辨率。

桌面端支持如下：

Windows：Edge uwp 版 Netflix 4K，其他全是 720，可通过插件支持 1080

macOS：safari 1080 其他全是 720，可通过插件支持 1080

Chrome OS：1080

电视看 Netflix：

第一关，是需要原生 IP，电视的 Netflix 的 IP 库识别要比手机严格。

第二关：获得较低的认证或没有认证的机器一般看不了 4k。当然，国产 ROM 就别说了。

第三关：你的电视支持硬件要求，外挂盒子的话需要，数据线需要支持 HDMI2.0 和 HDCP2.2（不知道准不准），，用 test pattern 可以看到分辨率。

土区车：Netflix 不限购买服务后的 IP，而土区因为汇率比较便宜，而这一般又是合租的，又称上车。

了解特殊服务需求的支持情况//购物/游戏解锁

6 参考及推荐链接

本文的编写过程，大量的参考了已有的文档，多数已注明出处，部分缺失的添加如下。

感谢以下博主 毒药博客 逗比根据地 rixCLoud Fndroid 关于策略组的理解 维基百科 Sukka's Blog SS/SSR 简介

以上文章，仅为个人观点，与其他作者无关。

需要说明的是，因为编辑器的原因，我插入维基百科的时候会有字符报错，所以我注明了出处，请千万不要用于商业用途，仅供个人查看。